A Rough Overview of MATH 103 **Van Wyk**

Updated 25 August 2008

Chapter One: Logic and Set Theory

- A *proposition* or *statement* is a sentence that is either true or false.
- Given propositions p and q, compound propositions can be formed using the following logical operations (each given by its defining truth table):
  - *negation* ($\sim$):

p	$\sim p$
T	F
F	T

  - *disjunction* ($\vee$):

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

  - *conjunction* ($\wedge$):

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

  - *implication* ($\Rightarrow$):

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

  - *biconditional* ($\Leftrightarrow$):

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

- Think of propositions p, q, r, etc. as "logical variables" that can take on the "logical values" T and F. Compare this with the "real variables" x, y, z, etc. that can take on any "real value."
- THE NEGATION OF AN IMPLICATION IS NOT AN IMPLICATION. In fact, the negation of $p \Rightarrow q$ is $p \wedge (\sim q)$, as you can verify with a truth table.
- *DeMorgan's Laws* state that the negation of a conjunction is a disjunction and vice-versa. More precisely, the negation of the proposition "$p \vee q$" is the proposition "$(\sim p) \wedge (\sim q)$" and the negation of the proposition "$p \wedge q$" is the proposition "$(\sim p) \vee (\sim q)$."

- Let $p \Rightarrow q$ be an implication. Its *hypothesis* is p, its *conclusion* is q, its *converse* is $q \Rightarrow p$ and its *contrapositive* is $(\sim q) \Rightarrow (\sim p)$. An implication is logically equivalent to its contrapositive. The negation of $p \Rightarrow q$ is $p \wedge (\sim q)$.

- There are two *quantifiers* for logical variables:

  - The *universal* quantifier, $\forall$, which is read "for each, "for all," "for every," etc.
  - The *existential* quantifier, $\exists$, which is read "for some," "for at least one," "there exists," etc.

  The negation of a universal quantifier is an existential quantifier, and vice versa. More precisely, the negation of the proposition "$\forall x, P(x)$" is the proposition "$\exists x$ such that $(\sim P(x))$", and the negation of the proposition "$\exists x$ such that $P(x)$" is the proposition "$\forall x, (\sim P(x))$".

Example. The negation of

> For all x, there exists a y such that $xy > 0$ or $x \geq y$.

is

> There exists an x such that for all y, $xy \leq 0$ and $x < y$.

- Analagous to the world of "propositions and logical operations" is the world of "sets and set operations." (We will assume the notion of a *set* is familiar.) If A and B are sets then A is a *subset* of B ($A \subseteq B$) if every element of A is also an element of B. Generally, we can assume we are working inside a fixed *universe of discourse* $\mathcal{U}$.

- Given sets A and B, we can form new sets using the following operations:

  - *complementation*: $A' = \{x \in \mathcal{U} \mid x \notin A\}$.
  - *union*: $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.
  - *intersection*: $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
  - *Cartesian product*: $A \times B = \{(x,y) \mid x \in A \text{ and } y \in B\}$.

- $|A \times B| = |A||B|$.

Example. If $\mathcal{U} = \{1,2,\ldots,99,100\}$, $A = \{33,34,\ldots,66\}$, and $B = \{50,51,\ldots,99,100\}$,

then

$$\begin{aligned}
A \cup B &= \{33, 34, \ldots, 99, 100\} \\
A \cap B &= \{50, 51, \ldots, 65, 66\} \\
A' &= \{1, 2, 3, \ldots, 32, 67, 68, \ldots, 99, 100\} \\
A \times B &= \{(33,50), (33,51), \ldots, (33,100), \\
&\quad (34,50), (34,51), \ldots, (34,100), \\
&\quad (35,50), (35,51), \ldots, (35,100), \\
&\quad \vdots \\
&\quad (66,50), (66,51), \ldots, (66,100)\}
\end{aligned}$$

□ There is an analogy between the logical operations and the set operations above. In particular,

Logical operation	Set operation
$\sim p$	A'
$p \vee q$	$A \cup B$
$p \wedge q$	$A \cap B$
$p \Rightarrow q$	$A \subseteq B$
$p \Leftrightarrow q$	$A = B$

Chapter Two: Number Theory

- An integer n *divides* an integer m, written $n|m$, if there exists some integer k such that $nk = m$.
- A positive integer is *prime* if it has exactly two divisors. A positive integer is *composite* if it has more than two divisors. Since 1 has only one divisor, it is neither prime nor composite.
- The *Fundamental Theorem of Arithmetic* states that any positive integer greater than one can be written uniquely (except for the order of the prime factors) as a product of primes.
- $n|m$ if and only if for every prime power p^k in the prime decomposition of n, there is at least the same power of p in the prime decomposition of m.
- Given two positive integers m and n, the *greatest common divisor* of m and n ($\gcd(m,n)$) and the *least common multiple* of m and n ($\text{lcm}(m,n)$) are defined in the obvious ways. (Listen to the words: "*greatest common* divisor" and "*least common* multiple.") If you know the prime factorizations of m and n, then you can get the prime factorization of $\gcd(m,n)$ by taking the smaller of the two exponents on each prime. You can also get the prime factorization of $\text{lcm}(m,n)$ by taking the larger of the two exponents on each prime. **Reminder:** $p^0 = 1$, so if a prime is not there, it has an exponent of 0.
- If n is a positive integer, then $d(n)$ denotes the *number* of divisors of n. If the prime factorization of n is

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r},$$

then

$$d(n) = (k_1+1)(k_2+1)(k_3+1)\ldots(k_r+1).$$

Example. If $m = 2^4 \cdot 3 \cdot 5^2$ and $n = 2^3 \cdot 3^2 \cdot 7$, then $\gcd(m,n) = 2^3 \cdot 3$, $\text{lcm}(m,n) = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7$, $d(m) = (5)(2)(3) = 30$, and $d(n) = (4)(3)(2) = 24$.

- If a and b are an integers with $b > 0$, then the *division algorithm* states that there exist integers q and r such that $a = bq + r$ with $0 \le r < b$. (q is the quotient and r is the remainder.)

Example. If $a = 287$ and $b = 5$, then $287 = 5 \cdot 57 + 2$, so $q = 57$ and $r = 2$.

- Integers (and, in fact any numbers) can be written in *base b* for any integer $b > 2$.

$$(a_n a_{n-1} \ldots a_2 a_1 a_0)_b \text{ means}$$

$$a_n b^n + a_{n-1} b^{n-1} + \cdots + a_2 b^2 + a_1 b + a_0.$$

Example. To convert 5032_{seven} to base ten, just use the above definition:

$$\begin{aligned} 5032_{\text{seven}} &= 5\cdot 7^3 + 0\cdot 7^2 + 3\cdot 7 + 2 \\ &= 5\cdot 343 + 21 + 2 \\ &= 1738_{\text{ten}} \end{aligned}$$

Example. If you wanted to count from one to twenty-five in base five, then you would write

$$\begin{array}{rrrrr} 1, & 2, & 3, & 4, & 10, \\ 11, & 12, & 13, & 14, & 20, \\ 21, & 22, & 23, & 24, & 30, \\ 31, & 32, & 33, & 34, & 40, \\ 41, & 42, & 43, & 44, & 100 \end{array}$$

Example. If you wanted to compute $3213_{\text{three}} + 303_{\text{three}}$, just line up the two numbers and add like you do in base ten, remembering that $4_{\text{ten}} = 10_{\text{four}}$, $5_{\text{ten}} = 11_{\text{four}}$, and $6_{\text{ten}} = 12_{\text{four}}$:

$$\begin{array}{ccccc} & 1 & & 1 & \\ & 3 & 2 & 1 & 3 \\ & & 3 & 0 & 3 \\ \hline 1 & 0 & 1 & 2 & 2 \end{array}$$

Example. To convert 1738_{ten} to base seven, you can do one of two things.

1. You can compute all the powers of 7 that are less than 1738: $7^0 = 1$, $7^1 = 7$, $7^2 = 49$, and $7^3 = 343$. ($7^4 = 2401$ is too big.)

   Then see how the multiples of these powers add up to 1738:

   - 343 goes into 1738 **five** times: $5\cdot 343 = 1715$.
   - You can't add any multiples of 49 to this sum, since $1715 + 49 = 1764 > 1738$, so 49 goes into this sum **zero** times.
   - 7 goes into this sum only **three** times since $1715 + 0 + 21 = 1736$, but $1715 + 0 + 28 = 1743 > 1738$.
   - 1 goes into this exactly **two** times, since $1715 + 0 + 21 + 2 = 1738$.

   Then since $1738 = \mathbf{5}\cdot 7^3 + \mathbf{0}\cdot 7^2 + \mathbf{3}\cdot 7^1 + \mathbf{2}\cdot 7^0$, $1738_{\text{ten}} = 5032_{\text{seven}}$ by definition.

2. You can also use the division algorithm repeatedly as follows, by repeatedly dividing the quotient by 7 until you get a quotient of 0:

   $$\begin{aligned} 1738 &= 7\cdot 248 + 2 \\ 248 &= 7\cdot 35 + 3 \\ 35 &= 7\cdot 5 + 0 \\ 5 &= 7\cdot 0 + 5 \end{aligned}$$

   Then write the remainders in reverse order to get $1738_{\text{ten}} = 5032_{\text{seven}}$.

   (This second method always works, but actually showing *why* it works is cumbersome.)

□ Converting between a base b and any power of that base b^k – in particular, converting between base two and base four, eight, or sixteen – can be done directly.

When converting from any base that is a power of two to binary, just rewrite each digit in binary. To go the other way, reverse the process.

Example. To convert $39B4_{\text{sixteen}}$ to base two, rewrite each of the four symbols $3, 9, B, 4$ in binary. Notice that $16 = 2^4$, so we will need four binary digits for each symbol. So, since three, nine, eleven, and four have binary representations 0011, 1001, 1011, and 0100, respectively, we have

$$39B4_{\text{sixteen}} = 0011\ 1001\ 1011\ 0100_{\text{two}}.$$

Example. To convert 11100001_{two} to base eight, subdivide the digits into groups of three (since $8 = 2^3$), working right to left, and write the number 0–7 that corresponds with each group. So

$$\begin{aligned} 11100001_{\text{two}} &= 011\ 100\ 001_{\text{two}} \\ &= 341_{\text{eight}}. \end{aligned}$$

Chapter Three: Probability

- The *sample space* S of an *experiment* is the set of all possible *outcomes*. An *event* E is a subset of S. The *probability* of E is

$$P(E) = \frac{|E|}{|S|}.$$

Example. Suppose your experiment is "roll a pair of dice" and your event E is "the sum of the numbers on the dice is 6." Then $S = \{1,2,3,4,5,6\} \times \{1,2,3,4,5,6\}$, so $|S| = 36$. Also $E = \{(1,5),(2,4),(3,3),(4,2),(5,1)\}$, so $|E| = 5$. Therefore $P(E) = \frac{5}{36}$.

- Two events E and F are
  - *mutually exclusive* if $E \cap F = \emptyset$. So, if E and F are mutually exclusive, then $P(E \cap F) = 0$.
  - *independent* if $P(E \cap F) = P(E)P(F)$.
- Axioms of probability include the following:
  - For any event E, $0 \leq P(E) \leq 1$.
  - $P(E') = 1 - P(E)$.
  - If E and F are mutually exclusive, then $P(E \cup F) = P(E) + P(F)$.
- If E and F are any events in the same sample space, then

$$P(E \cup F) = P(E) + P(F) - P(E \cap F).$$

- The *Fundamental Counting Principle* states that the number of ways to perform k independent tasks is the *product* of the number of ways to perform each of the tasks separately.

Example. Suppose you have to label chairs in a classroom with one letter and one integer between 1 and 1000. Then there are $26 \cdot 1000 = 26000$ different labels.

Example. How many different numbers have a binary representation of ten digits? Well, each of the ten digits has two possibilities (0 and 1), so there are $2^{10} = 1024$ different numbers.

- If n is a natural number, then *n factorial* is the number

$$n! = (n)(n-1)(n-2)\dots(3)(2)(1).$$

  By definition, $0! = 1$.

Example. $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$.

- There are two ways to choose r objects from n objects without replacement.

– If the order in which you choose *doesn't* matter, then compute the number of *combinations of n things taken r at a time*,

$$ {}_nC_k = \frac{n!}{k!(n-k)!}. $$

– If the order in which you choose *does* matter, then compute the number of *permutations of n things taken r at a time*,

$$ {}_nP_k = \frac{n!}{(n-k)!}. $$

Example. A club has 15 members. The number of ways to pick a president, vice-president, secretary, and treasurer is ${}_{15}P_4 = \frac{15!}{11!} = 15 \cdot 14 \cdot 13 \cdot 12 = 32760$, while the number of ways to pick four members to serve on a committee is ${}_{15}C_4 = \frac{{}_{15}P_4}{4!} = \frac{15 \cdot 14 \cdot 13 \cdot 12}{4 \cdot 3 \cdot 2} = 1365$.

Example. In a lottery, the goal is to choose a set of six numbers out of the numbers $1, 2, 3, \ldots, 50$. The number of possible ways to choose six numbers out of this set is ${}_{50}C_6 = \frac{50!}{44!6!} = 15,890,700$. Since there is only one choice that wins the lottery, the probability of winning this lottery is $\frac{1}{15,890,700}$, or about 0.000006%. (Not too good.)

Chapter Four: Geometry

- There are four types of *rigid motions of the plane* (or just "motions"): *rotation* (about a point), *reflection* (about a line), *translation* (in a certain direction a certain distance), and *glide reflection* (a translation followed by a reflection about a line parallel to the direction of the translation).
- A *symmetry* of a plane figure is a motion that places the figure back onto itself.
- The symmetry types of finite figures (those which encompass a finite area) are
  - *rotational* or *cyclic* symmetry types:

    $$C_1, C_2, C_3, \ldots$$

    A figure of type C_n has a minimum rotation of $\frac{360}{n}$ degrees. (C_1 has no symmetry.)
  - *reflective* or *dihedral* symmetry types:

    $$D_1, D_2, D_3, \ldots$$

    A figure of type D_n has n lines of symmetry. Since the product of two reflections about lines that intersect is a rotation, types D_n for $n \geq 2$ also have rotational symmetry (with a minimum rotation of $\frac{360}{n}$ degrees, twice the angle between two adjacent lines of reflection.)

Example. Here are four figures:

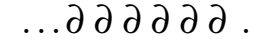
$$\exists \quad \partial \quad \S \quad \otimes$$

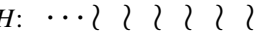
$\exists$ has a horizontal line of symmetry and no others, so it is type D_1. ∂ has no symmetry, so it is type C_1. § has half-turn symmetry only, so it is type C_2. $\otimes$ has exactly four lines of symmetry (horizontal, vertical, and both diagonals), so it is type D_4; notice it also has quarter-turn symmetry.

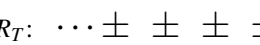
- There are seven symmetry types of *frieze patterns* or *border patterns*. (The adjective "certain" should be placed before all motions below. For example, when it says "invariant under translations," it means "invariant under certain translations.")
  - Type T, which is invariant under translations only. (Notice that *all* frieze patterns are invariant under translations.)
  - Type TH, which is invariant under translations and half-turns.
  - Type TR_T, which is invariant under translations and transverse reflections.
  - Type TR_L, which is invariant under translations and longitudinal reflections.
  - Type TG, which is invariant under translations and glide-reflections.

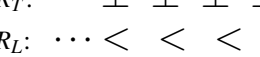
- Type TR^2, which is invariant under translations, transverse reflections, and longitudinal reflections (and hence half-turns and glide reflections).
- Type TRG, which is invariant under translations, transverse reflections, and glide reflections (and hence half-turns).

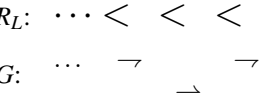
Example. Here is an example of each type.

Type T: 

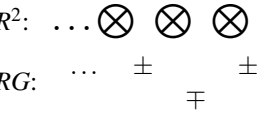
Type TH: 

Type TR_T: 

Type TR_L: 

Type TG: 

Type TR^2:

Type TRG: 

□ A plane motion is *direct* if it preserves the *sense* (or *orientation*) of figures; it is *opposite* if it reverses the sense of figures.

□ Direct (D) and opposite (O) motions "multiply" just like positive and negative numbers:

	D	O
D	D	O
O	O	D

So a product of motions is direct if and only if there are an even number of opposite motions; a product of motions is opposite if and only if there are an odd number of opposite motions.

□ A *fixed point* of a plane motion is a point that is not moved by the motion. A motion with no fixed points is called *fixed-point free*.

□ We have the following:

	has fixed points	fixed-point free
direct	rotations	translations
opposite	reflections	glide reflections

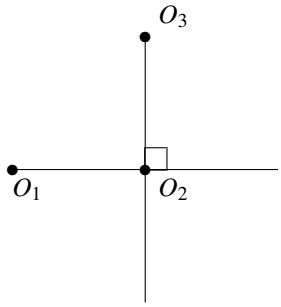
□ *Every* rigid motion of the plane can be written as a product of at most 3 reflections. So *every* rigid motion of the plane must be a rotation, reflection, translation, or glide reflection; there are no others. To determine which kind of motion it is, answer two questions:

1. Is the motion direct or opposite?
2. Does the motion have fixed points?

□ Determining if a motion is direct or opposite is easy; determining whether or not it has fixed points can be hard. Here is a helpful way to determine which of the four types of motion an unknown motion can be:

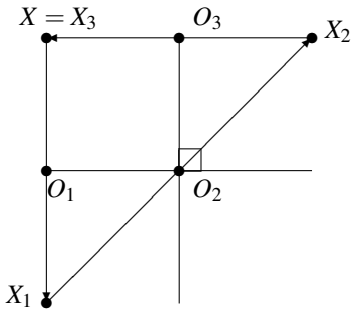
- Suppose the motion is direct.
  - ∗ If all the points in the plane move the same distance in the same direction, then the motion must be a *translation*.
  - ∗ If at least two points don't move the same distance in the same direction, then the motion must be a *rotation*.
    Furthermore, you can find the center of rotation by finding the point of intersection of two perpendicular bisectors of "before" and "after" points (say $\overline{XX'}$ and $\overline{YY'}$).
- Suppose the motion is opposite.
  - ∗ If all the points in the plane move parallel to each other (either in the same or opposite directions), then the motion must be a *reflection*.
    Furthermore, you can construct the axis of reflection by connecting the midpoints of two "before" and "after" points (say $\overline{XX'}$ and $\overline{YY'}$).
  - ∗ If at least two points don't move parallel to each other, then the motion must be a *glide reflection*.
    Furthermore, you can construct the glide axis by connecting the midpoints of two "before" and "after" points (say $\overline{XX'}$ and $\overline{YY'}$).

Example. In the figure below, let H_1 be a half-turn about point O_1, let H_2 be a half-turn about point O_2, and let H_3 be a half-turn about point O_3. What type of motion is the product $H_1H_2H_3$?



Since all three component motions are direct, the product $H_1H_2H_3$ is direct, so it must be either a translation or a rotation.

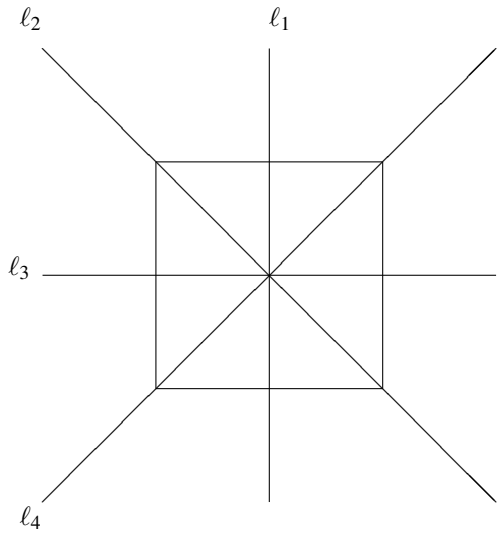
Also, the point X below is a fixed point of $H_1H_2H_3$: H_1 sends X to X_1, H_2 then sends X_1 to X_2, and H_3 then sends X_2 to $X_3 = X$. So $H_1H_2H_3$ must be a *rotation* about X.



In fact, $H_1H_2H_3$ is a *half-turn* about X. You can see this by following the point O_1 as you apply $H_1H_2H_3$: it ends up directly *above* O_1 on the other side of X (try it), so the angle of rotation is 180°.

□ A *regular* n-gon is a polygon with n sides for which all sides and all angles are equal. The symmetry type of a regular n-gon is D_n, and each D_n is called a *dihedral group*; it has $2n$ elements. Each element of D_n sends the n-gon back onto itself.

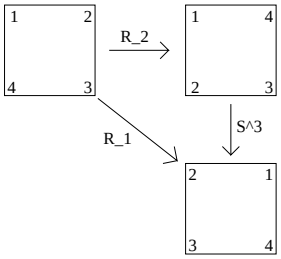
Example. The symmetry group of the square is $D_4 = \{I, S, S^2, S^3, R_1, R_2, R_3, R_4\}$, where R_i is a reflection about the line ℓ_i below, $S = R_1R_2$ is a counterclockwise rotation of 90°, and I is the "identity element" which represents doing nothing to the square.



Notice the rotations I, S, S^2, S^3 are all direct motions while the reflections R_1, R_2, R_3, and R_4 are all opposite motions. So, the product of two rotations must be a rotation, the product of two reflections must be a rotation, and the product of a rotation and a reflection (in either order) must be a reflection.

You can compute all 64 possible products of elements of D_4 by hand. For example, the following diagram shows that the product R_2S^3 has the same result as

the single motion R_1, so $R_2S^3 = R_1$. (Note: the numbers are to keep track of the square.)



Below is the entire table for D_4, which contains all 64 possible products of its elements. You always do the elements down the left column first, and the elements along the top row second. For example, R_1R_2 is S, while R_2R_1 is S^3. Notice $R_1R_2 \neq R_2R_1$, so the order you do these products in can effect the outcome.

	I	S	S^2	S^3	R_1	R_2	R_3	R_4
I	I	S	S^2	S^3	R_1	R_2	R_3	R_4
S	S	S^2	S^3	I	R_4	R_1	R_2	R_3
S^2	S^2	S^3	I	S	R_3	R_4	R_1	R_2
S^3	S^3	I	S	S^2	R_2	R_3	R_4	R_1
R_1	R_1	R_2	R_3	R_4	I	S	S^2	S^3
R_2	R_2	R_3	R_4	R_1	S^3	I	S	S^2
R_3	R_3	R_4	R_1	R_2	S^2	S^3	I	S
R_4	R_4	R_1	R_2	R_3	S	S^2	S^3	I

Also notice the four basic types of products from the table:

$$\begin{aligned}
(\text{rotation})(\text{rotation}) &= \text{rotation},\\
(\text{rotation})(\text{reflection}) &= \text{reflection},\\
(\text{reflection})(\text{rotation}) &= \text{reflection, and}\\
(\text{reflection})(\text{reflection}) &= \text{rotation}.
\end{aligned}$$

Chapter Five: Group Theory

- A *binary operation* $*$ on a set S is a rule that assigns to each ordered pair (x,y) of elements of S exactly one element of S, $x*y$.
- If $|S| = n$, then there are n^{n^2} different binary operations on S, one for each possible table.
- Let $*$ be a binary operation on S.
  - $*$ is *associative* if for all $a,b,c \in S$, $a*(b*c) = (a*b)*c$.
  - $*$ is *commutative* if for all $a,b \in S$, $a*b = b*a$.
  - $e \in S$ is an *identity* under $*$ if for all $a \in S$, $a*e = e*a = a$.
  - If $*$ has an identity e, then $a,b \in S$ are *inverses* if $a*b = b*a = e$. (**Notation:** $b = a^{-1}$.)
- **Remarks.** $*$ is commutative iff its multiplication table is symmetric about the main diagonal. Associativity is hard to check, in general. An operation which is associative but not commutative is *left projection*: $\square * \bigcirc = \square$.

Example. Let $S = \{a,b,c\}$.

1. The binary operation $*$ given by the table

$*$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

   is associative (it is "right projection") but not commutative (since $b*c = c$, while $c*b = b$). There is no identity, so it doesn't make sense to talk about inverses.

2. The binary operation $\odot$ given by the table

$\odot$	a	b	c
a	a	c	b
b	c	c	b
c	b	b	a

   is commutative (since the table is symmetric about the main diagonal) but not associative (since $b\odot(b\odot c) = b\odot b = c$, while $(b\odot b)\odot c = c\odot c = a$). There is no identity, so it doesn't make sense to talk about inverses.

3. For the binary operation $\oslash$ given by the table

$\oslash$	a	b	c
a	a	c	a
b	c	a	b
c	a	b	c

   c is the identity (therefore c is its own inverse). a and b are inverses of each other.

- □ Since the left and right cancellation laws hold for groups, every *group* table contains every element exactly once in each row and in each column.
- □ If G is a group and $S \subseteq G$, then S is *closed* if $a * b \in S$ whenever $a, b \in S$.
- □ If $H \subseteq G$, then H is a *subgroup* of G, written $H \leq G$, if H is itself a group. In fact, $H \leq G$ iff
  - H is closed.
  - The identity is in H.
  - H has all its own inverses.
- □ If $H \leq G$, then a (left) *coset* of H is a set of the form $a * H = \{a * h \mid h \in H\}$ for some $a \in G$.
- □ *Lagrange's Theorem* states that (for a finite group G) if $H \leq G$ then $|H|$ divides $|G|$.

Example. Here is the table for a group G:

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	d	c	a	f	e
c	c	f	a	d	e	b
d	d	b	f	e	c	a
f	f	c	e	b	a	d

1. The set $S = \{b, c\}$ is not closed because $b \circ c = a \notin S$. (There are other reasons too.)
2. The set $T = \{e, c, d\}$ is closed; all possible products result in elements of T:

$\circ$	e	c	d
e	e	c	d
c	c	d	e
d	d	e	c

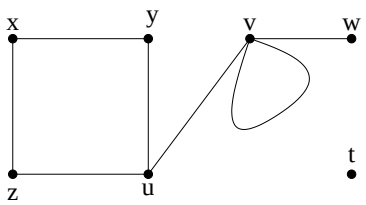
   Since $e \in T$ and T contains all its inverses (c and d are inverses of each other), T is a subgroup of G.
3. Since $|T| = 3$ and $|G| = 6$, the subgroup T has 2 cosets. One, as always is T, which is also $e \circ T = c \circ T = d \circ T$. The other coset, $\{a, b, f\}$, is $a \circ T = b \circ T = f \circ T$.

Example. If G has a prime number of elements, then the only subgroups of G are $\{e\}$ and G, since the only divisors of $|G|$ are 1 and $|G|$. So groups with a prime number of elements have no "interesting" subgroups.

Chapter Six: Graph Theory

- A *graph* consists of *vertices* and *edges* which run between vertices. If there is an edge between two vertices, they are *adjacent*, and both of the vertices are *incident* with that edge. A *loop* is an edge from a vertex to itself.
- The *degree* of a vertex is the number of edges incident with it, loops counting twice. (Equivalently, it is the number of parts of edges sticking out of the vertex.) The degrees of all the vertices can be summarized in an *adjacency matrix*.

Example. The following is a graph with 7 vertices (labeled) and 7 edges, one of which is a loop at v:



The degree of each vertex is

vertex	degree
x	2
y	2
z	2
u	3
v	4
w	1
t	0

w is a *pendant* vertex and t is an *isolated* vertex.

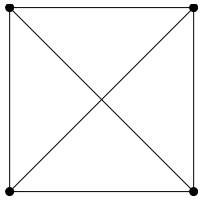
The adjacency matrix for this graph is

	x	y	z	u	v	w	t
x	0	1	1	0	0	0	0
y	1	0	0	1	0	0	0
z	1	0	0	1	0	0	0
u	0	1	1	0	1	0	0
v	0	0	0	1	1	1	0
w	0	0	0	0	1	0	0
t	0	0	0	0	0	0	0

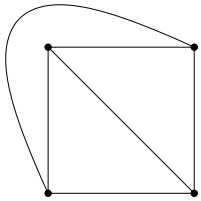
Notice the adjacency matrix is symmetric about the main diagonal.

- A *plane* graph is a graph with no edge crossings. A *planar* graph can be drawn with no edge crossings. There are planar graphs that are not plane graphs.

Example. Here is a planar graph that is not a plane graph:



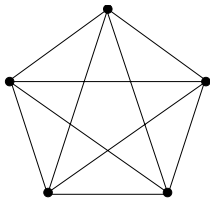
To see that it is planar, redraw it as:



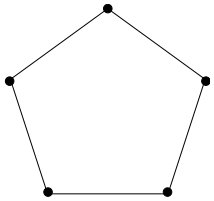
- A *simple* graph is a graph with no loops or multiple edges.
- Three important classes of simple graphs are:
  1. The *complete* graph, K_n. Every pair of the n vertices is adjacent.
  2. The *cyclic* graph, C_n. This is simply an n-sided polygon.
  3. The *complete bipartite* graph, $K_{n,m}$. The vertices are split into two disjoint sets, one with n elements and one with m. Every vertex in the one set is adjacent to every vertex in the other set, and no other vertices are adjacent.

Example.

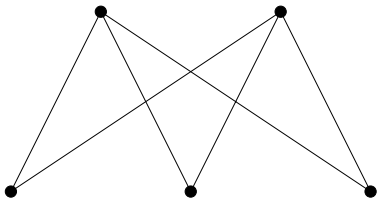
1. Here is K_5:



2. Here is C_5:

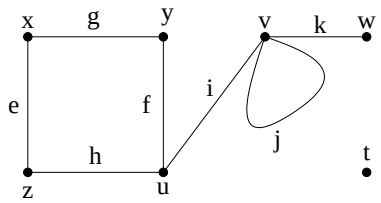


3. Here is $K_{2,3}$:



□ The concept of a *path* in a graph is exactly what you would guess, with the requirement that a path begins at a vertex and ends at a vertex. A path is *closed* or a *circuit* if it begins and ends at the same vertex. If it isn't closed, it is *open*. The length of a path is the number of edges it traverses.

Example. In the following graph



an open path from z to w of length 6 is

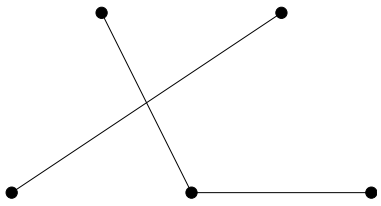
$$z \xrightarrow{h} u \xrightarrow{f} y \xrightarrow{f} u \xrightarrow{i} v \xrightarrow{j} v \xrightarrow{k} w$$

while a closed path at u of length 3 is

$$u \xrightarrow{i} v \xrightarrow{j} v \xrightarrow{i} u.$$

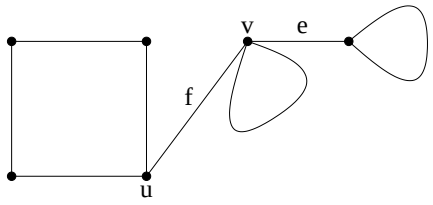
□ A graph Γ is *connected* if there is a path connected any two of its vertices. If Γ is not connected, then the maximum connected subgraphs of Γ are its *connected components*.

Example. The following graph has two components, one containing two vertices and the other containing the other three vertices.



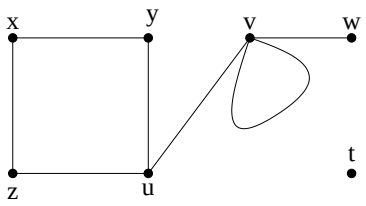
□ A *cut vertex* of a graph Γ is a vertex v such that $\Gamma - \{v\}$ has more components than Γ. A *cut edge* of a graph Γ is an edge e such that $\Gamma - \{e\}$ has more components than Γ.

Example. In the following graph, u and v are cut vertices, while e and f are cut edges:



□ The *Handshaking Theorem* states that in any graph Γ with E edges, the sum of the degrees of all the vertices of Γ is $2E$. This is easy to see, since each edge contributes 2 to the total degree of the graph.

Example. In the graph in the example of degree of a vertex,



the sum of the degrees is

$$2+2+2+3+4+1+0=14,$$

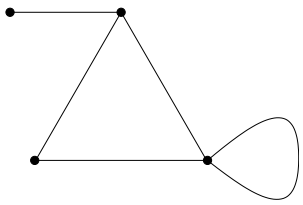
and the number of edges is 7.

□ If Γ is a connected plane graph, then it splits the plane up into *faces*, one of which is "exterior" (or "unbounded" or "infinite").

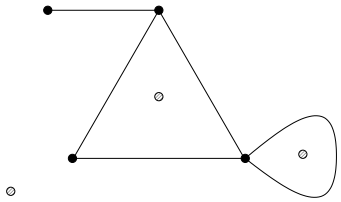
□ If Γ is a connected plane graph, then its *dual graph* Γ^* has

- a vertex f^* for every face f of Γ.
- an edge e^* for every edge e of Γ such that the vertices f_1^* and f_2^* of Γ^* are connected by the edge e^* in Γ^* exactly when the faces f_1 and f_2 are separated by the edge e in Γ.

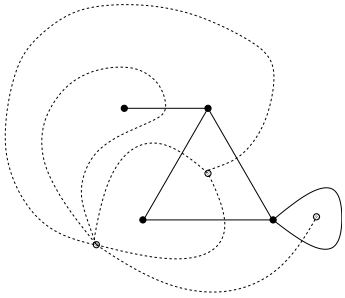
Example. Here is a plane graph Γ with three faces (the inside of the triangle, the inside of the loop, and the exterior face):



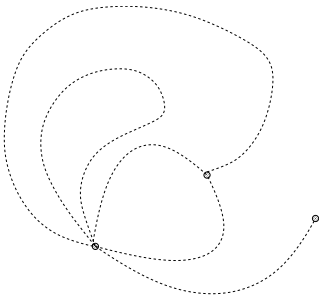
To form its dual graph Γ^*, first put a vertex in each of the three faces:



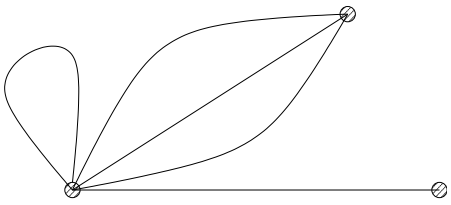
Then connect every two new vertices with an edge if their corresponding faces in Γ are separated by an edge in Γ:



If we draw Γ^* alone, we get



We can redraw Γ^* to look a bit nicer:



Notice that Γ^* is also planar. Furthermore,

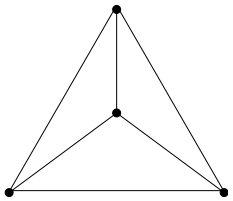
	Γ	Γ^*
# vertices	4	3
# edges	5	5
# faces	3	4

The roles of "vertex" and "face" have been interchanged. That is what duality is all about in graph theory.

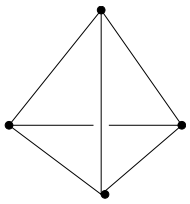
Also, if we started with Γ^* (drawn in the original way, not starting with the "redrawn" Γ^*) and formed *its* dual, we would get Γ back again. In other words, $(\Gamma^*)^* = \Gamma$.

□ If Γ is a plane graph, it can be embedded on a sphere (in a "3-dimensional way"). When this is done, the exterior face becomes just another bounded face.

Example. Start with the following plane representation of K_4 (3 bounded faces, 1 unbounded face):



This can be redrawn as a tetrahedron with 4 bounded (2-dimensional) faces:



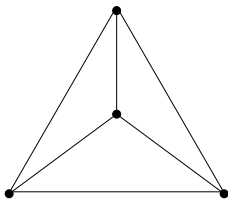
□ An *edge path* in a graph Γ is a path that traverses each edge of Γ exactly once.

□ A graph Γ is *Eulerian* if it has a closed edge path.

□ We know exactly when a graph has an open or closed edge path:

- Γ is Eulerian if and only if Γ is connected and all the vertices of Γ have even degree.
- Γ has an open (but not closed) edge path if an only if Γ is connected and exactly two of its vertices have odd degree.

Example. K_4 has neither an edge circuit nor an edge path since it has four vertices of odd degree:



□ If G is a group and $X \subseteq G$, then X is a *generating set* for G if every element of G can be written as a "product" of the elements of X and their inverses. These products are called "words" in X.

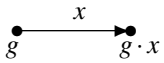
Example. The group $\mathbb{Z}_5$ is generated by the single element $\{2\}$ because

$$\begin{aligned} 1 &= 2+2+2 \\ 2 &= 2 \\ 3 &= 2+2+2+2 \\ 4 &= 2+2 \\ 0 &= 2+2+2+2+2 \end{aligned}$$

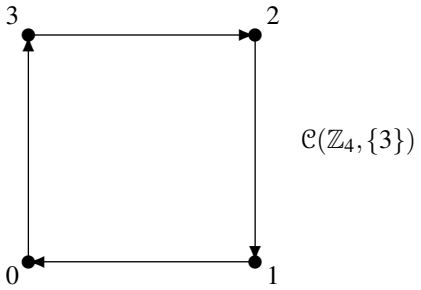
Example. We showed in class that D_4 is generated by the subset $\{S, R_1\}$.

□ If G is a group and $X \subseteq G$, then the *Cayley graph* of G with respect to X, $\mathcal{C}(G,X)$, is the directed graph with

- **Vertices.** The elements of G.
- **Edges.** For all $g \in G$ and for all $x \in X$,



Example. The Cayley graph of $\mathbb{Z}_4$ with respect to the generating set $X = \{3\}$ is:



Here each of the edges is labeled "3".

- In any Cayley graph:
  - The graph is connected.
  - Every vertex has an edge going in and an edge going out for every element of X.
  - So, every vertex has the same degree.
- A Cayley graph gives a "picture" of a group.

THE END